UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/505,830	02/17/2000	Christian L. Houlberg	82 100	6929

7590 05/21/2004	EXAMINER
Commander	SEAL, JAMES
Office of Counsel 772000E	

ART UNIT	PAPER NUMBER
2135	

Commander
Office of Counsel 772000E
Navairwarcenwpndiv
521 9th Street
Point Mugu, CA 93042-5001

DATE MAILED: 05/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No. 09/505,830		**Applicant(s)** HOULBERG ET AL.
Office Action Summary	**Examiner** James Seal		**Art Unit** 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
   Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _05 April 2004_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _6,7,9,11,13 and 16_ is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _6,7,9,11,13 and 16_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   This Action is in reply to applicant's correspondence of 05 April 2004.

2.   Amendments to the specification page 5, page 7 lines 1 and lines 22 have been entered.

3.   Amendment to abstract has been entered.

4.   Claim 1-5, 8, 10, 12, and 14-15 have been cancelled without prejudice.

5.   Claims 6-7, 9, 11, 13, and 16 are pending.

Oath/Declaration

6.   The Oath/Declaration received 05 April 2004 has been enter.

7.   Amendments to the Specification have been entered and the examiner withdraws his objection.

8.   With the new Abstract, the objections to the abstract are withdrawn.

Claim Objections

9.   Claim 11 is objected to because of the following informalities: Claim 11 refers to a cancelled claim 10. Appropriate correction is required. For the purpose of the application of prior art the examiner will assume that claim 11 refers to claim 6.

Claim Rejections - 35 USC § 103

10.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11.   Claims 6-7, 9, 11, 13, and 16 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Borgen H1414, and further in view of Maher 5513261 A, Wade WO

98/07099, and Best 4465901 A.

12.   As per claim 6, the limitation for providing a crypto key (or key) from a key

loader is taught by Borgen (Column 2, line 7 and Column 13, line 33, note the KOI-18,

KYK-13 and the KYK-15A are well known key loaders used by the military), and

providing a checkword (i.e. test word, key word or digital word) may be stored in the

nonvolatile memory system see Column 2, lines 7) to an nonvolatile memory (Column

2, lines 11-12) for a telemeter system missile is disclosed by Borgen (Column 1, lines

15-30). Borgen thus teaches storing a checkword or key into nonvolatile memory but

is silent with regards to their association.

13.   Maher teaches the use of the checkword together (associated) with the key as a

method of validating the transfer of key material from a portable source such as a card

or key loader to a host machine the checkword being used to validate the key that was

transferred (Column 4, lines 1-7, figure 2). Thus it would have been obvious for one of

ordinary skill in the art at the time the invention had been made to have loaded the key

and checkword (therefore associated) from the loader to the nonvolatile memory

because the checkwork could validate the key transfer and hence make the transfer

process more secure.

14.   The limitation of a microcontroller connected to the key loader as a monolithic

device is not disclosed by Borgen or Maher as their embodiment teach separate

memory and control elements (see Borgen, Column 2, lines 16-21). Wade teaches a

monolithic microcontroller including internal memory and I/O (Figure 1). Wade discuses

the many advantages of the microprocess with its internal memory (see especially page

1, lines 19-24. Thus it would have been obvious to one of ordinary skill in the art at the

time the invention was to have replaced the external memory, I/O of the Borgen circuit

with a monolithic microcontroller because of lower fabrication costs and higher

reliabilities and in addition storing the key in the internal memory of the microcontroller

provides better security than transfers between devices.

15.   The limitation that microcontroller connected to the key loader to receive the

crypto key and associated checkword from the keyloader is then disclosed by the

Borgen/Wade reference (in Borgen Column 13, lines 26-37 indicates loader, which may

be a model number KOI-18, or KYK-13 or KYK-15A key loaders and Figure 1B element

276 indicates key loader) loads key/digital word into (Borgen Column 2, line 7) into

nonvolatile memory (Borgen Column 2, lines 7 element 332 Figure 1B) of the

microcontroller's internal memory disclosed by Wade see figure 1. The microcontroller

sending a first variable request signal to the key loader to effect a transfer to the

microcomputer's internal memory (Borgen Column 16 lines 44-67 and Column 17 lines

1-8, indicate the process of transferring the key/digital word from the loader to RAM 78

and Column 19 lines 17-33 and in particular VARREQ output control sequence to the

loader indicated to the loader that the RAM 76 is ready to receive data). connected to

the encryption device such that controller sends a second logic signal to said encryption

device to *initiate a load* of cryptokey and associated checkwork into encryption device is disclosed by Borgen Column 18, lines 24-25.

16.   The limitation that the microcontroller including (see discussion above) an internal EEPROM (note the internal memory unit element 14 in Wade can accomodate of many types of non-volatiles types, page 7, lines 21-27, including EEPROM flash EEPROM as well as static SRAM cells. It would have been obvious for one of ordinary skill in the art at the time that the invention was made to have upgraded the logic chips including the EEPROM332 Figure 1b to be included in the microcontroller of Wade see figure 1 element 14 and figure 2 element 34) because internal memory is more secure faster, lower fabrication costs and higher reliabilities see page 1 Wade. The limitation of making a copy of the key material (key and checkword) is not disclosed by Borgen/Wade/Maher combination. Best disclose transferring information from the key loader into memory and generating copies of the key material as well as making copies available to the encryptor (see Column 14, lines 29-31). It would have obviously to one of ordinary skill in the art at the time that the invention was made to have made copies in the case the original keys were corrupted later.

17.   The limitation that the microcontroller that the microcontroller is connected to the encryption device (see Figure 1b, elements 288 and 75) sending a sense in signal to the encryptor (Column 16, lines 48-49) to initiate load of key material into encryptor (Column 20, lines 22-31).

18.   The limitation that the microcontroller receiving from a variable request signal
and responsive to this signal the from the encryptor the microcontroller sends key
material to the encryptor is disclosed by Borgen (Column 20, lines 32-50).

19.   The limitation that the microcontroller being connected to a transmitter for the
telemeter system of said missile, said microcontroller providing a transmitter disable
signal to the transmitter to disable transmitter when key material is loaded into the
encryptor.

20.   Borgen/Wade/Best/Maher are silent on disabling the transmitter circuitry while
downloading the key, however, one of ordinary skill in the art at the time the invention
was made would have been motivated to disable any transmitter circuit because any
open circuit to the outside world would provide a path for accidental transmission of the
key material leading to compromise of data if not caught and certainly would be
TEMPEST noncompliance.

21.   The limitation of providing software programs for controlling handling and
interpreting, transfer key material from the key loader to the internal EEPROM and
within the EEPROM of the microcontroller, and from thence to the encryptor, testing and
finally enabling the transmitter after successful loading of the encryptor is a software
implementation of the apparatus as recited above and the same prior art applies to the
software implementation. Claim 6 is rejected.

22.   With regards to claims 7, the limitation that the microcontroller comprises an 8-bit
microcontroller is disclosed by Wade. Wade disclose both 8 and 16 bit controllers and
thus it would have been obvious for one of order skill in the art at the time the invention

was made to have picked either implementation for the implementation of the rest of the electronics which in the case of Borgen would have been 8-bits.

23.   Claim 8 is cancelled.

24.   As per claim 9, the limitation of an LED visual indicator connected to the microprocessor to indicate the status of the key material into the encryption device. Borgen/Wade/Best/Maher combination is silent as to whether status information is displayed by LED or otherwise, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have to have used a low power LED as a visual indicator of the success or failure of the download of the key material into the encryptor before telemetry was transmitted because it was lessen the likelihood of compromise of classified material. That the LED is connected to a controller is also obvious as it is the device that loads and transfers data. Claim 9 is rejected.

25.   Claim 10 has been cancelled.

26.   As per claim 11, the Borgen/Wade/Best/Maher combination is silent as to whether an LED is used to indicate whether the key material has been erased from memory, however, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have use an LED indicator light as a visual means to determine if the previous key material were erase to prevent detection of the previously stored key material in RAM (Column 20, lines 59-63). Claim 11 is rejected.

27.   Claim 12 is cancelled.

28.   Claim 13 recites the limitations of claim 6 with the additional limitations that the microcontroller is 8 bit (Claim 7)with a first LED to indicate the status of the download

into the encryptor (Claim 9) and a second LED to indicate the status of the erasure of

key material from memory (claim 11). It would have been obvious for one of ordinary

skill in the art at the time the invention was made to have combined the last two reason

with the recited invention in 6 because of security and the 8 bit microcontroller from

Wade because it would then be compatible with the rest of the Borgen circuit. Claim 13

is rejected.

29.   Claims 14-15 are cancelled.

30.   As per claim 16, the limitation wherein the microcontroller is connected to the

loader interface to receive an erase signal from loader interface, erasing key material

from microcontoller is disclosed by Borgen Column 22, lines 31-40. The limitation of

making a copy of the key material (key and checkword) is not disclosed by

Borgen/Wade/Maher combination. Best disclose transferring information from the key

loader into memory and generating copies of the key material as well as making copies

available to the encryptor (see Column 14, lines 29-31). It would have obviously to one

of ordinary skill in the art at the time that the invention was made to have made copies

in the case the original keys were corrupted later

31.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Response to Arguments

32.   Applicant's arguments filed 05 April 2004 have been fully considered but they are

not persuasive.

33.   In response to applicant's argument that the examiner's conclusion of

obviousness is based upon improper hindsight reasoning, it must be recognized that

any judgment on obviousness is in a sense necessarily a reconstruction based upon

hindsight reasoning. But so long as it takes into account only knowledge which was

within the level of ordinary skill at the time the claimed invention was made, and does

not include knowledge gleaned only from the applicant's disclosure, such a

reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA

1971). The examiner note the SIR appears to be based on Borgen Master Thesis, at

the University of California, Santa Barbara 1989, in which microcontroller technology

was still in its infancy (see Wade page 1). It may be the case that Borgen's design

based on 1989 technology would incorporate gates and logic circuits (with truth tables),

complex electronic design and hard wired digital logic circuitry as separately

components as would have still been in fashion in 1989, but by the mid 90s Wade

discloses that microcontroller technology is the ideal replacement for such technology (Wade page 1 and 2). Generally new technology does allow more flexibility such as incorporation of static and dynamic memory. That it requires redesign taking advantage of the technology does not make it non-obvious. Wade gives many of the advantages for gate technology with microcontrollers. Microcontroller allow one to do things that 1989 technology does not such as in packing, speed, flexibility etc.

34.   In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Maher was brought in as it associates the key with the checkword (or digital word) as an integral part of the transfer procedure. It allows validation of the key material that is transferred. Borgen uses the key word = digital word (see Column 13, lines 49-50 and again Column 20 44-55 where the key word is transferred to the encryptor and the stored results are sent to a comparator) for checkword but it carries the same meaning.

Conclusion

35.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.
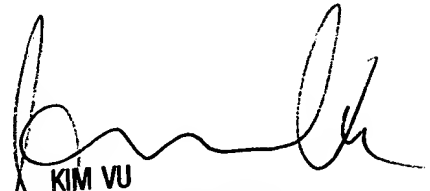
If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Jws

14 May 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100